EXHIBIT 1

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

COMMODITY FUTURES TRADING COMMISSION, Plaintiff, v. CONTROL-FINANCE LIMITED AND BENJAMIN REYNOLDS, Defendants.	ECF Case No. 19-cv-5631 **COMPLAINT FOR INJUNCTIVE AND OTHER EQUITABLE RELIEF AND FOR CIVIL MONETARY PENALTIES UNDER THE COMMODITY EXCHANGE ACT AND COMMISSION REGULATIONS**

Plaintiff Commodity Futures Trading Commission (the "Commission"), by and through counsel, alleges as follows:

I. INTRODUCTION

1. Since at least May 1, 2017, through the present, Defendant Control-Finance Limited ("Control-Finance") and its sole Director, Defendant Benjamin Reynolds ("Reynolds"), (together, "Defendants"), exploited public enthusiasm for Bitcoin by operating a fraudulent scheme to misappropriate at least 22,858.822 Bitcoin—which reached a valuation of at least $147 million—from more than 1,000 members of the public ("customers").

2. From at least May 1 through October 31, 2017 (the "Relevant Period"), Defendants fraudulently solicited customers to purchase their own Bitcoin with cash and thereafter deposit their Bitcoin with Defendants. To facilitate these transactions, Defendants included hyperlinks to virtual currency processors (entities that buy and sell Bitcoin) on the main page of their public website, www.control-finance.com (the "Control-Finance Website").

3. To entice customers to transfer Bitcoin to them, Defendants falsely represented that they employed expert virtual currency traders who earned guaranteed daily trading profits on customers' Bitcoin deposits.

4. To create the false impression that Defendants were successfully trading customers' Bitcoin deposits in virtual currency markets, Defendants fabricated weekly "Trade Reports" and posted them to the Control-Finance Website. The Trade Reports reflected illusory virtual currency transactions and profits, when in reality Defendants made no trades on customers' behalf and earned no trading profits for them.

5. Defendants also manufactured an aura of profitability by diverting portions of new customers' Bitcoin deposits to other customers in the manner of a "Ponzi" scheme, falsely representing that these misappropriations were in fact profits derived from virtual currency trading.

6. Defendants' fraud was not limited to touting non-existent virtual currency trading and profits. Rather, Defendants used the Control-Finance Website, as well as social media websites including Facebook, YouTube, and Twitter, to construct an elaborate pyramid scheme they called the Control-Finance "Affiliate Program." Through the Affiliate Program, Defendants fraudulently promised to pay, in the form of Bitcoin, escalating referral profits, rewards, and bonuses to "Affiliates"—consisting of any person who requested a referral hyperlink, regardless of whether he or she was an existing customer—based on the number of new customers they referred to Defendants.

7. Throughout the Relevant Period, Defendants used the Control-Finance Website and social media to entice Affiliates to use their own social media accounts on websites including YouTube, Facebook, and Twitter, among others, to advertise Control-Finance's

purported virtual currency trading returns, to distribute referral hyperlinks to new customers, and to alleviate customers' apprehension by reporting that Defendants had been paying them Bitcoin returns on their deposits.

8. On or around September 10, 2017, Defendants, having fraudulently solicited at least 22,858.822 Bitcoin from customers, abruptly terminated operations by removing the Control-Finance Website from the Internet, halting payments to customers and Affiliate Program members, and deleting advertising content from Defendants' Facebook, YouTube, and Twitter accounts.

9. To deceive customers into believing that Control-Finance was only temporarily inactive and that customers' Bitcoin deposits were safe and secure, Defendants fraudulently represented through email and Facebook that Defendants would make all customers whole by returning their Bitcoin deposits, minus any prior payments, by late October or November 2017.

10. In reality, Defendants had no intention of resuming operations and deliberately lulled customers into complacency while Defendants set to work laundering nearly one hundred fifty million dollars in misappropriated Bitcoin through thousands of circuitous blockchain transactions. Defendants routed the great majority of these transactions through wallet addresses that Defendants established at CoinPayments of Vancouver, Canada.

11. By this conduct, and as more fully alleged below, Defendants have engaged, are engaging in, and/or are about to engage in acts and practices in violation of the Commodity Exchange Act (the "Act"), 7 U.S.C. §§ 1-26 (2012), and its implementing Commission Regulations ("Regulations"), 17 C.F.R. pts. 1-190 (2018). In particular, Defendants violated Section 6(c)(1) of the Act, 7 U.S.C. § 9(1) (2012), and Regulation 180.1(a), 17 C.F.R. § 180.1(a) (2018).

12. Unless restrained and enjoined by this Court, Defendants are likely to continue to engage in the acts and practices alleged in this Complaint, and in similar illegal acts and practices.

13. Accordingly, pursuant to Section 6c of the Act, 7 U.S.C. § 13a-1 (2012), the Commission brings this action to permanently enjoin Defendants from further violations of the Act and Regulations and to seek civil monetary penalties and ancillary relief, including but not limited to permanent trading and registration bans, restitution, and disgorgement.

II. JURISDICTION AND VENUE

14. **Jurisdiction**. This Court possesses jurisdiction over this action pursuant to 28 U.S.C. § 1331 (2012) (codifying federal question jurisdiction) and 28 U.S.C. § 1345 (2012) (providing that U.S. district courts have original jurisdiction over civil actions commenced by the United States or by any agency expressly authorized to sue by Act of Congress). In addition, Section 6c(a) of the Act, 7 U.S.C. § 13a-1(a) (2012), provides that U.S. district courts have jurisdiction to hear actions brought by the Commission for injunctive relief or to enforce compliance with the Act whenever it shall appear to the Commission that any person has engaged, is engaging, or is about to engage in an act or practice constituting a violation of any provision of the Act or any rule, regulation, or order thereunder.

15. The Commission has anti-fraud authority over the conduct and transactions at issue in this action pursuant to Section 6(c)(1) of the Act, 7 U.S.C. § 9(1) (2012), and Regulation 180.1(a), 17 C.F.R. § 180.1(a) (2018).

16. **Venue**. Venue properly lies with this Court pursuant to Section 6c(e) of the Act, 7 U.S.C. § 13a-1(e) (2012), because acts and practices in violation of the Act occurred, are occurring, or are about to occur, within this District. Venue is appropriate in this district because

Defendants fraudulently solicited and misappropriated Bitcoin deposits from customers residing in this district.

III. THE PARTIES

17. Plaintiff **Commodity Futures Trading Commission** is an independent federal regulatory agency charged by Congress with the administration and enforcement of the Act and Regulations. The Commission maintains its principal office at 1155 21st Street N.W., Washington, DC 20581.

18. Defendant **Control-Finance Limited** is a now-defunct United Kingdom private limited company that was organized by Defendant Reynolds and incorporated by the Registrar of Companies for England and Wales (the "U.K. Registrar") on September 8, 2016. Control-Finance maintained its Registered Office in Manchester, United Kingdom. On February 20, 2018, the U.K. Registrar dissolved Control-Finance. Control-Finance has never been registered with the Commission in any capacity.

19. Defendant **Benjamin Reynolds** is an individual and United Kingdom national who resides in Manchester, England. On July 9, 2016, Reynolds submitted an application to the U.K. Registrar to incorporate Control-Finance as a U.K. private limited company. Reynolds was at all times Control-Finance's sole Director and at all times owned 100% of Control-Finance's 1,000 equity shares. On September 6, 2016, Reynolds registered in his own name the www.control-finance.com Internet domain name. Reynolds has never been registered with the Commission in any capacity.

IV. STATUTORY AND CONCEPTUAL BACKGROUND

20. Bitcoin is encompassed within the definition of "commodity" under Section 1a(9) of the Act, 7 U.S.C. § 1a(9) (2012).

21. For purposes of this Complaint, Bitcoin, like all virtual or "crypto" currencies, is a digital representation of value that functions as a medium of exchange, a unit of account, and/or a store of value, but does not have legal tender status in any jurisdiction. Bitcoin is distinct from "real" currencies, which are the coin and paper money of sovereign jurisdictions that are designated as legal tender, placed into circulation, and used and accepted as a medium of exchange within the country of issuance. In contrast, Bitcoin uses cryptographic protocols to secure transactions and relies on decentralized, peer-to-peer networks to track and confirm transactions between parties identified only by publicly-visible character strings.

22. Blockchain, a form of distributed ledger technology, underpins Bitcoin and many other virtual currencies. Blockchain transactions are captured in single "blocks" at a time, which independent operators (called "miners," a virtual analogue to actual miners whose efforts unearth precious metals) confirm by performing algorithmic proofs of work, in exchange for which they receive a sum of the virtual currency in question. The public nature of the decentralized ledger allows people to recognize the transfer of virtual currencies from one user to another without requiring any central intermediary that both users must trust.

23. For purposes of this Complaint, the term "wallet address" refers to a 26-35 digit alphanumeric public key that operates similarly to a bank account and can be used to send and receive Bitcoin and other virtual currencies. For readability, wallet addresses are identified in this Complaint by their last 4 digits (*see* paragraphs 68, 70-77, 81). While anyone can send virtual currency to a particular wallet address, transferring virtual currency out of a wallet address requires a private key held by the owner of the wallet address. Unlike bank accounts, wallet addresses are public information and are recorded on the blockchain for viewing by members of the public.

Case 1:19-cv-05631-MKV Document 34-1 Filed 08/20/20 Page 8 of 37

24. For purposes of this Complaint, the term "Altcoin" refers to any virtual currency other than Bitcoin.

V. FACTS

A. Operation of Defendants' Fraudulent Scheme

25. During the Relevant Period, Defendants operated a complex fraudulent scheme in which they solicited and misappropriated at least 22,858.822 Bitcoin from more than 1,000 customers, some of whom reside in this District. Defendants induced United States customers to purchase Bitcoin from third-party vendors and to thereafter transfer the Bitcoin to Defendants. Defendants' fraudulent scheme consisted of several components:

i. The Control-Finance Website

26. The nerve center of Defendants' fraudulent scheme was the Control-Finance Website, which Defendants at all times owned and controlled. The Control-Finance Website was registered with a United States Internet hosting company located in San Francisco, California. As alleged below, Defendants used the Control-Finance Website to make material misrepresentations and omissions to prospective and existing customers to entice them to open Control-Finance accounts and deposit their Bitcoin with Defendants.

27. Defendants also used the Control-Finance Website to provide customers with nominal, sham account balances and profit figures. In reality, the illusory account balances and profit statements that Defendants provided to customers were not backed up by actual Bitcoin, because Defendants had misappropriated the Bitcoin for their own use.

ii. Defendants' Social Media Accounts

28. Defendants at all times owned and controlled social media accounts, including accounts at YouTube, Facebook, Twitter, and LinkedIn (collectively and without limitation, the "Social Media Accounts").

29. Throughout the Relevant Period, Defendants used the Social Media Accounts to make material misrepresentations and omissions to customers and to entice customers to open Control-Finance accounts and deposit their Bitcoin with Defendants.

30. At various times during the Relevant Period, Defendants used the Social Media Accounts to advertise "contests" for the purpose of attracting new customers. For example, on July 7, August 4, and September 1, 2017, Defendants used the Control-Finance Facebook account to advertise "contests" whereby Facebook users were purportedly entered into a random drawing for Bitcoin "prize pools" if they "shared" Defendants' contests through their own Facebook accounts. Defendants operated these contests for the purpose of attracting new customers for Defendants to defraud.

iii. Email Communications

31. At all times, Defendants owned and controlled the admin@control-finance.com email address (the "Control-Finance Email Address"). Defendants used the Control-Finance Email Address to communicate directly with and solicit customers, including customers residing within this District.

32. Defendants used the Control-Finance Email Address to make false and fraudulent misrepresentations to customers about Defendants' trading methods, abilities, and profits.

33. On September 11 and 12, 2017, after Defendants abandoned their scheme, Defendants used the Control-Finance Email Address to falsely inform customers that their Bitcoin deposits were safe and secure and would be returned to them. Defendants knowingly made these and other false statements to customers for the purpose of lulling customers into complacency while Defendants completed their misappropriation of customers' Bitcoin deposits.

iv. The Control-Finance Affiliate Program

34. Throughout the Relevant Period, Defendants operated an "Affiliate Program" that relied on fraudulently offering outsized referral profits, rewards, and bonuses, paid in Bitcoin, to encourage both customers and others to refer new customers to Defendants.

35. Defendants operated the Affiliate Program by using the Control-Finance Website to generate referral hyperlinks that Affiliates could send to friends and family members and post publicly on the Internet, often with commentary advertising the supposed trading profits, rewards, and bonuses to be had by depositing Bitcoin with Defendants.

36. The referral hyperlinks directed new customers to the Control-Finance Website, where they could view Defendants' material misrepresentations and omissions and were encouraged to deposit Bitcoin with Defendants. Each time a new customer clicked on a referral hyperlink and deposited Bitcoin through the Control-Finance Website, Defendants "rewarded" the Affiliate by creating a nominal Bitcoin credit in the Affiliate's Control-Finance Account.

37. Defendants, in an effort to ensnare as many victims as possible and in the manner akin to a pyramid scheme, used the Affiliate Program to provide referral hyperlinks to anyone who requested one, even if the requestor had not personally deposited any Bitcoin with Defendants.

38. Defendants also offered special "VIP" benefits to higher-level Affiliates called "Representatives," which Defendants defined as Affiliates who had themselves deposited at least $300 worth of Bitcoin with Defendants. Defendants used purported "VIP" benefits, including special access to Defendant Reynolds via online "chat" sessions, as well as other "rewards" and "bonuses," to entice customers to become Representatives by depositing Bitcoin with Defendants.

39. Defendants also publicly offered downloadable website "banners," which Affiliates could publicly post on social media websites and in online public forums. The banners contained embedded referral hyperlinks that redirected to the Control-Finance Website, where new customers could view Defendants' material misrepresentations and omissions, open Control-Finance accounts, and deposit Bitcoin with Defendants.

40. Defendants' fraudulent scheme relied on exploiting the Affiliate network to widely advertise Control-Finance through social media, public websites, face-to-face interactions, and word-of-mouth, for the purpose of directing as many customers as possible to open accounts with Defendants, regardless of the size of each investment. By targeting huge numbers of victims, Defendants were able to fraudulently solicit Bitcoin deposits worth at least $147 million despite requiring a minimum deposit of only $10 worth of Bitcoin.

v. Sham Account Balances

41. Customers who were enticed to deposit Bitcoin with Defendants were provided a deposit confirmation webpage through the Control-Finance Website. Each deposit confirmation webpage identified the quantity of Bitcoin deposited and the value of that Bitcoin in U.S. dollars. In addition, each deposit confirmation webpage identified the daily "Profit" that Defendants promised to pay to customers on each deposit. Finally, each deposit confirmation webpage

stated that profit "Reinvestment" was available, and that profits could be withdrawn "at any time."

42. Contrary to the daily profit percentages stated in the deposit confirmation webpages, Defendants had no intention of actually paying profits or returns to the vast majority of customers. Rather, Defendants almost immediately misappropriated customers' deposits by routing them to new wallet addresses that Defendants controlled.

43. To conceal their misappropriation, Defendants used the Control-Finance Website to generate automated profit credits that accrued in customers' accounts each day. While customers' Control-Finance accounts falsely reflected growing balances, in reality those accounts were empty.

44. Defendants also intentionally and recklessly used the profit "Reinvestment" option to create disincentives to account withdrawals, allowing Defendants to misappropriate greater quantities of customers' Bitcoin. By offering customers the option to reinvest their "profits" into a program that on its surface appeared to be highly profitable, Defendants concealed and prolonged their fraud by convincing customers that their deposits were rising in value, causing customers to leave their deposits in their Control-Finance accounts rather than request withdrawals.

45. In instances where customers did request withdrawals from their Control-Finance accounts, Defendants illegally diverted Bitcoin deposited by other customers to satisfy the withdrawal requests.

Case 1:19-cv-05631-MKV Document 34-1 Filed 08/20/20 Page 13 of 37

B. Specific Fraudulent Solicitations

i. Material Misrepresentations and Omissions Concerning Trading, Profits, and Accounts

46. Throughout the Relevant Period, Defendants intentionally and recklessly used the Control-Finance Website and the Social Media Accounts to make material misrepresentations and omissions about Defendants' virtual currency trading methods, abilities, and profits, as well as customers' account security and their ability to withdraw purported profits. Defendants knowingly made these and other material misrepresentations and omissions with the intent to solicit prospective and existing customers to transfer their Bitcoin to Defendants.

47. Defendants intentionally and recklessly made the following material misrepresentations, among others, to prospective and existing customers:

a. Throughout the Relevant Period, Defendants publicly represented the following on the "Trade reports" webpage of the Control-Finance Website: "Our team consists of professional traders using the following currency pairs: BITCOIN/USD, ETH/BITCOIN, ETC/BITCOIN, LTC/USD, and other Altcoins. *All of our clients' funds are used in real trading activities without exception.*" (Emphasis added). These representations were false and fraudulent because Defendants knew that they did not employ professional traders, that they did not use customers' deposits for trading, that they did not obtain Altcoins on customers' behalf, and that Defendants misappropriated customers' deposits.

b. Throughout the Relevant Period, Defendants publicly advertised "Investment Offer" solicitations on the Control-Finance Website, guaranteeing returns "for [the] lifetime" of each deposit, and at various times bonus payments of 3% or 5% interest on each deposit. These representations were false and fraudulent because

Case 1:19-cv-05631-MKV Document 34-1 Filed 08/20/20 Page 14 of 37

Defendants knew that customers' deposits did not earn profits, that customers did not receive interest bonus payments on their deposits, that customers' Control-Finance accounts reflected sham balances and profit statements that were not supported by underlying Bitcoin, and that Defendants misappropriated customers' deposits.

c. Throughout the Relevant Period, Defendants publicly represented the following on the Control-Finance LinkedIn account: (i) "*Control Finance 45% per month – Up to 1.5% every single day.*"; and (ii) "Control Finance Investment. *You get a profit up to 1.5% every single day!*" (Emphasis added). These representations were false and fraudulent because Defendants knew that customers did not earn 1.5% daily or 45% monthly profits, that customers' account balances and profit statements were a sham, and that Defendants misappropriated customers' deposits.

d. Throughout the Relevant Period, Defendants used the Control-Finance Facebook account to fraudulently solicit customers by, among other things, posting the following on the account's "About" webpage: "*Earn 1.5% every single day.* Passive income. Bitcoin Investment. Trade Reports." (Emphasis added). These representations were false and fraudulent because Defendants knew that customers did not earn 1.5% daily profits, that customers earned no passive income on their deposits, that customers' account balances and profit statements were a sham, and that Defendants misappropriated customers' deposits.

e. On June 23, 2017, Defendants used the Control-Finance Website to publicly advertise supposed account security enhancements, writing, "Control Finance

takes care of the funds of each client. *We focus not only on generating profit but also on preserving your investments.*" (Emphasis added). These representations were false and fraudulent because Defendants knew that they did not generate profits for customers, that they did not take any action to preserve customers' investments, and that Defendants misappropriated customers' deposits.

f. On July 19, 2017, Defendants used the "News" section of the Control-Finance Website to publicly address supposed customer concerns about an anticipated bifurcation, or "fork," within the Bitcoin market. Defendants described Control-Finance as a "safe haven" amidst market changes, representing that Control-Finance provided customers with "risk diversification and proper allocation of your assets." Defendants further represented, "[o]ur company's balance is calculated in US dollars, so we recommend that you invest right now, and you will be protected from possible bifurcation in the blockchain network." These representations were false and fraudulent because Defendants knew that they provided no "risk diversification," "proper allocation," or other protection from Bitcoin market effects or bifurcations, and that Defendants misappropriated customers' deposits.

g. On July 21, 2017, Defendants used the "News" section of the Control-Finance Website to publicly represent: "Our specialist team of traders has developed a secure scheme for working with cryptocurrency exchanges, applying a diversification method by increasing the number of trading accounts on new cryptocurrency exchanges such as Bitfinex, Bitsamp and Okcoin." These representations were false and fraudulent because Defendants knew that they did

Case 1:19-cv-05631-MKV Document 34-1 Filed 08/20/20 Page 16 of 37

not employ a specialist team of traders, that they took no action to develop a secure scheme for working with cryptocurrency exchanges, and that they applied no diversification methods to manage customers' Bitcoin deposits.

h. On September 6, 2017, Defendants published a YouTube video in which an unidentified man, visible in an office setting displaying the Control-Finance logo on the wall, broadcast the misrepresentations identified in paragraph 47.g. above. The man in the YouTube video concluded by saying, "I am taking this opportunity to invite others to join. Go ahead and sign up now. We make money here." The representations Defendants made in the September 6, 2017, YouTube video were false and fraudulent for the reasons alleged in paragraph 47.g. above.

48. Throughout the Relevant Period, Defendants used the Control-Finance Website and the Social Media Accounts to make material omissions to prospective and existing customers about Defendants' purported virtual currency trading abilities, methods, and profits, including, among other things, by failing to disclose that: (i) Defendants misappropriated customers' Bitcoin deposits; and (ii) purported trading profits and returns paid to certain customers were in fact the misappropriated principal deposits of other customers.

49. Defendants intentionally and recklessly made all of the material misrepresentations and omissions alleged in paragraphs 46-48 for the purpose of executing and concealing their fraud and enticing prospective and existing customers to transfer Bitcoin to Defendants.

ii. Fabricated Weekly Trade Reports

50. Throughout the Relevant Period, Defendants used the Control-Finance Website to publicly advertise fabricated weekly "Trade Reports" that fraudulently represented profitable virtual currency trades that Defendants never placed.

51. In addition to fabricating virtual currency trading data, the Trade Reports contained material misrepresentations and omissions that Defendants disguised as market analysis and used to entice prospective and existing customers to transfer their Bitcoin to Defendants. For example, the Trade Report for the period of July 3 through July 9, 2017, represented in part:

> We observed Bitcoin exiting correction territory for short-terms during the previous trading week. Meanwhile Litecoin-related forecasts also scored. We successfully traded other altcoins as well. The current period is not the simplest for crypto currencies market [sic] because of Segwit implementation and the fact that July is traditionally not the most successful month for trading. But even in this situation we continue demonstrating stable results with a total profitability of 2-3% per day.

These representations were false and fraudulent because Defendants knew that they did not trade virtual currencies on customers' behalf, they did not achieve trading profits of 2-3% per day, and that Defendants misappropriated customers' deposits.

52. As another example, the Trade Report for the period of July 17 through July 23, 2017, represented in part:

> This trading week was full of events. The entire global cryptocurrency community followed the news about Bitcoin's hard fork—the so-called SigWit2x. What did that give us? – Volatility! This is a great time for trading. As we reported earlier, our orders in the range of 1800-1950 worked and we had an excellent and lucrative week thanks to good news.

These representations were false and fraudulent because Defendants knew that they did not trade virtual currencies on customers' behalf, they did not have an "excellent and lucrative week" trading virtual currencies, and that Defendants misappropriated customers' deposits.

53. Defendants' Trade Report for the period of July 17 through July 23, 2017, also attempted to reassure customers that their deposits were safe. Defendants wrote, "I would like to again remind our customers to *please not worry. Your money is safe.* The only possible problem is that we may have unscheduled days off on July 31 and August 1 because of suspension of trading on cryptocurrency exchanges." (Emphasis added). These representations were false and fraudulent because Defendants knew that customers' money and Bitcoin deposits were not safe, that customers' Control-Finance accounts were empty, and that Defendants misappropriated customers' deposits.

54. Defendants intentionally and recklessly made all of the material misrepresentations alleged in paragraphs 50-53 for the purpose of executing and concealing their fraud and enticing prospective and existing customers to transfer Bitcoin to Defendants.

iii. Material Misrepresentations and Omissions Concerning the Affiliate Program

55. Throughout the Relevant Period, Defendants intentionally and recklessly used the Control-Finance Website and the Social Media Accounts to make material misrepresentations about the Control-Finance Affiliate Program. Defendants made these material misrepresentations to prospective and existing customers for the purpose of soliciting them to transfer their Bitcoin to Defendants, and to entice them to use the Internet, social media, face-to-face interactions, and word-of-mouth to market Control-Finance to other victims.

56. Defendants intentionally and recklessly made the following material misrepresentations, among others:

a. Throughout the Relevant Period, Defendants publicly advertised the Control-Finance Affiliate Program on the Control-Finance Website by writing: (i) "Open an account and start earning a passive income daily. *The activity of your referrals will guarantee you a comfortable livelihood.*"; and (ii) "Already got your affiliate team? *Then prepare to see your profit skyrocket!*" (emphasis added). These representations were false and fraudulent because Defendants knew that the Affiliate Program did not provide passive income or profits to customers, could not "guarantee" a livelihood, and that Defendants misappropriated customers' deposits.

b. Throughout the Relevant Period, Defendants publicly advertised the Control-Finance Affiliate Program on the Control-Finance Website by promising to pay escalating Bitcoin returns, rewards, and bonuses to reward Affiliates for bringing greater numbers of new customers to Defendants. Defendants' representations about escalating Bitcoin returns, rewards, and bonuses were false and fraudulent because Defendants had no intention of actually paying most Affiliates the promised returns, rewards, and bonuses, and that Affiliates' Control-Finance accounts nominally reflected sham balances that did not in fact exist.

c. Throughout the Relevant Period, Defendants used the Control-Finance Website to provide Affiliates with downloadable website "banners" containing embedded hyperlinks. Defendants encouraged Affiliates to post the banners on Internet websites and social media to direct new customers to the Control-Finance Website. Defendants also displayed material misrepresentations on the banners for the purpose of enticing Internet users to click on them. Among other material

Case 1:19-cv-05631-MKV Document 34-1 Filed 08/20/20 Page 20 of 37

misrepresentations, Defendants' banners represented the following: (i) "EARN UP TO 1.5% DAILY!"; and (ii) "REAL COMPANY WITH REAL TRADING." These representations were false and fraudulent because Defendants knew that customers' deposits did not earn up to 1.5% daily profits and that Defendants did not conduct any trading on customers' behalf.

d. On July 13, 2017, Defendants used the Control-Finance Website to publicly represent:

> In response to numerous requests made by our partners, we deployed the 1st planned upgrade to our affiliate program. Now you will receive affiliate remuneration in full for every deposit replenishment made by your referral. Now it has become even more profitable for you to invest your profit and bonuses.

These representations were false and fraudulent because Defendants knew that Affiliates would not receive remuneration for their referrals' deposits, that investing profits and bonuses back into Control-Finance would not create any profits for Affiliates, and that Affiliates' account balances and profit statements were shams.

e. Throughout the Relevant Period, Defendants used the Control-Finance Website and the Social Media Accounts to make material omissions to prospective and existing customers about the Affiliate Program, including, among other things, by failing to disclose that: (i) Defendants misappropriated customers Bitcoin deposits; and (ii) purported trading profits and returns paid to some customers were actually the misappropriated principal deposits of other customers.

57. Defendants intentionally and recklessly made all of the material misrepresentations and omissions alleged in paragraphs 55-56 for the purpose of executing and

concealing their fraud and enticing prospective and existing customers to transfer Bitcoin to Defendants.

iv. Fraudulent Email Communications

58. Throughout the Relevant Period, Defendants used the Control-Finance Email Address to make materially false misrepresentations and omissions to customers. At all times, Defendants owned and controlled the Control-Finance Email Address.

59. By way of example, when customers opened Control-Finance accounts, Defendants used the Control-Finance Email Address to contact customers with account login details and to write the following: "Now you have the unique opportunity to make a profit on transactions in the lucrative cryptocurrency market and earn passive income from our affiliate program." These representations were false and fraudulent because Defendants knew that customers did not earn profits on cryptocurrency transactions with Defendants, that customers did not earn passive income from the Affiliate Program, and that Defendants misappropriated customers' deposits.

60. Throughout the Relevant Period, Defendants used the Control-Finance Email Address to notify customers that Defendants had posted Trade Reports, which Defendants fabricated, to the Control-Finance Website. By way of example, on August 19, 2017, Defendants used the Control-Finance Email Address to contact Customer D.S., a U.S. resident, with the following message: "We posted Company's [sic] weekly trade report covering the period August 07, 2017, to August 13, 2017. You can have a look at it [sic] clicking on the following link. . . ." Defendants' purpose in sending this email, and others like it, was to direct customers to visit the Control-Finance Website, to view Defendants' fabricated Trade Reports, and to be fraudulently enticed to deposit additional Bitcoin with Defendants.

Case 1:19-cv-05631-MKV Document 34-1 Filed 08/20/20 Page 22 of 37

61. Defendants intentionally and recklessly made all of the material misrepresentations and omissions alleged in paragraphs 58-60 for the purpose of executing and concealing their fraud and enticing prospective and existing customers to transfer Bitcoin to Defendants.

D. Defendants' Misappropriation Scheme

62. Defendants used the Control-Finance Website as a conduit to receive Bitcoin deposits from customers and to then misappropriate those deposits in at least two ways: (i) by executing circuitous blockchain transactions that misappropriated customers' Bitcoin deposits by moving Bitcoin into other wallet addresses under Defendants' control; and (ii) by illegally diverting customers' Bitcoin deposits to make Ponzi scheme-like payments to other customers who requested withdrawals from their own Control-Finance accounts.

63. During the Relevant Period, Defendants misappropriated at least 22,858.822 Bitcoin from customers.

i. Single-Use Addresses and Pool Addresses

64. Defendants' misappropriation scheme relied on creating unique, single-use wallet addresses ("Single-Use Address(es)") to receive customers' Bitcoin deposits. In most cases, Defendants used each Single-Use Address for one pair of transactions: (i) to receive a Bitcoin deposit from a customer, and (ii) to route the customer's deposit to one of a number of pooled wallet addresses ("Pool Address(es)") into which Defendants transferred misappropriated Bitcoin from hundreds of Single-Use Addresses. At all times, Defendants owned, controlled, and operated the Single-Use Addresses and the Pool Addresses.

65. Defendants typically created a new Single-Use Address for every customer deposit. In typical transactions, customers logged into the Control-Finance Website and

accessed the deposit webpage. The Control-Finance Website then generated a unique Single-Use Address for the specific deposit. After a customer deposited Bitcoin with the Single-Use Address, Defendants routed the deposit out of the Single-Use Address and into a Pool Address, where the deposit was combined with numerous deposits by other customers. Defendants then misappropriated the Bitcoin in each Pool Address by transferring it to other wallet addresses under Defendants' control, including wallet addresses held at CoinPayments of Canada, Bithumb and Coinone of South Korea, Shapeshift of Switzerland, and Remitano of Seychelles.

66. Defendants' misappropriation strategy relied on obfuscation. To make it difficult for customers to track the movement of their Bitcoin deposits through the blockchain, Defendants typically executed "split" payments when transferring customers' Bitcoin out of Single-Use Addresses and into Pool Addresses. To execute a split payment, Defendants transferred the great majority of a customer's Bitcoin deposit out of a Single-Use Address and into a Pool Address. Defendants simultaneously transferred the remainder of the customer's Bitcoin deposit out of the Single-Use Address and into another wallet address that held a relatively small Bitcoin balance.

67. To execute their misappropriation scheme, on May 28, 2017, Defendants established User ID *294 at virtual currency payment processor CoinPayments of Vancouver, Canada. Defendants used CoinPayments User ID *294 to establish at least 45 Pool Addresses into which Defendants funneled 22,190.542 misappropriated Bitcoin from Single-Use Addresses.

68. In addition to the wallet addresses that Defendants established under CoinPayments User ID *294, Defendants created Pool Addresses at several other virtual currency payment processors and exchanges, including BTC-e of Russia, Huobi of Singapore, and Korbit of South Korea. During the Relevant Period, Defendants used these Pool Addresses

to misappropriate at least 668.28 Bitcoin from customers by transferring 90.348 Bitcoin into BTC-e Pool Address *Np4s, 554.943 Bitcoin into Huobi Pool Addresses *CBLw and *QeW6, and 22.989 Bitcoin into Korbit Pool Address *xYpm.

69. In total, Defendants misappropriated at least 22,858.822 Bitcoin from customers during the Relevant Period.

ii. CoinPayments Address *uk1x

70. Of the Pool Addresses that Defendants established under CoinPayments User ID *294, one in particular was central to Defendants' misappropriation scheme: CoinPayments Address *uk1x, through which Defendants misappropriated 5,184.65 Bitcoin from customers. At all times, Defendants owned, controlled, and operated CoinPayments Address *uk1x.

71. During the Relevant Period, Defendants used CoinPayments Address *uk1x in at least two ways: (i) as a Pool Address, in that Defendants used CoinPayments Address *uk1x to receive misappropriated Bitcoin from numerous Single-Use Addresses, and (ii) as a repository for consolidating misappropriated Bitcoin deposits from other Pool Addresses.

72. During the Relevant Period, Defendants transferred misappropriated Bitcoin from at least the following five Pool Addresses into CoinPayments Address *uk1x: *b2p5, *Tebs, *Q4DM, *fhB2, and *qEpB.

73. Throughout the Relevant Period, Defendants often executed circuitous blockchain transactions to move misappropriated Bitcoin into CoinPayments Address *uk1x. These transactions had no valid business purpose and were designed solely to obfuscate the illegal movement of customers' Bitcoin. The following transaction is an example of Defendants' efforts to obscure their misappropriation scheme:

a. On August 21, 2017, Defendants initiated blockchain transaction *adcc, which resulted in 59 Single-Use Addresses transferring a total of 62.488 Bitcoin to Pool Address *b2p5.

b. Immediately thereafter, Defendants initiated blockchain transaction *996c, which routed the 62.488 Bitcoin just received by Pool Address *b2p5 into two transactions: (i) 50.018 was transferred to CoinPayments Address *uk1x; (ii) 12.469 was transferred to wallet address *x9uc.

c. Immediately thereafter, Defendants executed blockchain transaction *2fcb, which resulted in 12.467 Bitcoin transferring from wallet address *x9uc into wallet address *W8KA.

d. Immediately thereafter, Defendants executed blockchain transaction *9b6a, which resulted in 12.972 Bitcoin transferring from wallet address *W8KA into CoinPayments Address *uk1x (constituting the 12.467 Bitcoin received by wallet address *W8KA plus an additional .505 Bitcoin).

74. While Defendants easily could have directly transferred Bitcoin from Pool Address *b2p5 to CoinPayments Address *uk1x—as they did with the initial 50.018 Bitcoin transfer—they chose instead to pay additional transaction fees to achieve the same result by executing the transfer in a roundabout fashion via transaction *2fcb and transaction *9b6a. These uneconomical transactions served no purpose other than masking Defendants' misappropriation of customers' Bitcoin via CoinPayments Address *uk1x.

75. Defendants' transfers of Bitcoin from Pool Address *b2p5 to CoinPayments Address *uk1x were only a part of Defendants' misappropriation scheme. Throughout the Relevant Period, Defendants intentionally and recklessly executed numerous circuitous

transactions when routing misappropriated Bitcoin from Single-Use Addresses and Pool Addresses to CoinPayments Address *uk1x. Defendants deliberately obfuscated their illegal transfers of Bitcoin into CoinPayments Address *uk1x for the purpose of concealing their fraud and making it more difficult for customers to track the movement of their misappropriated Bitcoin across the blockchain.

76. Throughout the Relevant Period, Defendants routed misappropriated Bitcoin out of CoinPayments Address *uk1x and into dozens of other wallet addresses. Upon information and belief, Defendants then withdrew or spent customers' misappropriated Bitcoin for Defendants' own benefit.

77. By August 23, 2017, Defendants had emptied the contents of CoinPayments Address *uk1x by executing blockchain transaction *80ab, which transferred the last 39.407 Bitcoin remaining in CoinPayments Address *uk1x to 31 separate wallet addresses. During the Relevant Period, Defendants used CoinPayments Address *uk1x to misappropriate a total of 5,184.659 Bitcoin from customers.

iii. Fraudulent Ponzi Payments

78. Throughout the Relevant Period, Defendants misappropriated customers' Bitcoin deposits by making Ponzi scheme-like payments to customers who requested withdrawals from their Control-Finance accounts.

79. Defendants' use of Ponzi scheme-like payments was central to Defendants' fraudulent scheme. Defendants intentionally and recklessly made these payments to customers to create the illusion that Control-Finance was profitable, to conceal Defendants' fraud, and to alleviate customers' apprehension about depositing Bitcoin with Defendants.

80. In addition, Defendants intentionally and recklessly made Ponzi scheme-like payments to Affiliates for the purpose of motivating Affiliates to represent on social media websites including YouTube, Facebook, Twitter, and Reddit that Defendants honored withdrawal requests and paid profits to Affiliates and customers. Defendants' intent in making these payments was to extend and conceal their fraud and to entice prospective and existing customers to deposit Bitcoin with Defendants.

81. The following transaction illustrates the process by which Defendants misappropriated customers' Bitcoin deposits to satisfy account withdrawal requests:

a. On or around September 7, 2017, Customer B.C., a U.S. resident, and the owner(s) of at least 58 other wallet addresses, logged into the Control-Finance Website and initiated Bitcoin withdrawals from their Control-Finance accounts.

b. To satisfy the withdrawal requests, Defendants on the same day initiated blockchain transaction *3743, which transferred 0.617 Bitcoin from three wallet addresses—*N5DY, *bpxc, and *Uvdp—to wallet address *hL1M ("Ponzi Address *hL1M"). At all times, Defendants owned, controlled, and operated Ponzi Address *hL1M.

c. Defendants obtained the 0.617 Bitcoin that Defendants transferred to Ponzi Address *hL1M through transaction *3743 by diverting the principal deposits of customers.

d. Two hours after the 0.617 Bitcoin was received by Ponzi Address *hL1M, Defendants initiated blockchain transaction *d072, which emptied Ponzi Address *hL1m by distributing its entire balance—0.617 Bitcoin—to the 59 customers who requested account withdrawals.

e. Ponzi Address *hL1M has only ever performed two transactions: receiving 0.617 Bitcoin and distributing it to the withdrawing customers.

E. Defendants Terminate Operations

82. On or around September 10, 2017, Defendants suddenly terminated their fraudulent scheme by shutting down the Control-Finance Website, suspending all payments to customers, and removing the majority of content from the Social Media Accounts.

83. To lull customers into believing that the shutdown was temporary and that customers' Bitcoin deposits with Defendants were safe, on September 11 and 12, 2017, Defendants falsely represented to customers via email and Facebook that Defendants' accounts had been temporarily frozen, but that all customer deposits were safe and would be returned by the end of October or early November 2017.

84. On September 11, 2017, Defendants used the Control-Finance Email Address to contact customers and assert that an unspecified "exchange" had "temporarily blocked" Defendants' ability to process account withdrawal requests. The email further stated that Defendants' attorneys were working to unblock Defendants' accounts, and further that Defendants were "establishing an algorithm for automated processing" of payments. The email concluded by writing, "we guarantee that we'll fulfill our obligations given to our customers," and that Defendants would soon "continue our stable growth to high profits as we always did in our company."

85. The representations Defendants made in the September 11, 2017, email to customers were false and fraudulent because Defendants knew that they would not implement an automated payment processing algorithm, that an exchange did not block Defendants' funds or accounts, that Defendants had no intention of ever returning customers' Bitcoin deposits, that

Defendants had never generated stable growth or profits for customers, and that Defendants misappropriated customers' funds.

86. On September 12, 2017, Defendants used the Control-Finance Email Address to contact customers and assert that Defendants' attorneys had "received information about the conditions for unblocking all trading accounts of the company," and that customers would soon receive the return of their Bitcoin deposits, minus any prior profit withdrawals. The email further stated that the Control-Finance Website "will temporarily stop working, but all customer databases with their payment and contact details will be stored on a separate server of the company . . . ." The email concluded by stating that the first customer payments were made on September 11, 2017, and "will continue, until the end of October."

87. The representations Defendants made in the September 12, 2017, email to customers were false and fraudulent because Defendants knew that Defendants had no intention of ever returning customers' Bitcoin deposits or account balances to them, that Defendants had no intention of making further payments to customers, and that Defendants had no intention of ever resuming operations.

88. On September 15, 2017, Defendants publicly posted Defendants' September 12, 2017, email message to customers on the Control-Finance Facebook page. For the reasons identified in paragraph 87 above, the Defendants' Facebook post of September 15, 2017, was false and fraudulent.

89. Contrary to the representations Defendants made to customers via email and Facebook on September 11, 12, and 15, 2017, Defendants had no intention to, and did not, resume operations or return customers' Bitcoin deposits.

Case 1:19-cv-05631-MKV Document 34-1 Filed 08/20/20 Page 30 of 37

90. Defendants' intent in sending the emails of September 11 and 12, 2017, and in making the Facebook post of September 15, 2017, was to lull customers into complacency by falsely representing that customers' deposits were safe and that temporary technical and regulatory barriers had merely delayed customers' withdrawal requests. Defendants intentionally and recklessly made these misrepresentations with the intent to reduce customers' scrutiny of Defendants' fraud and to afford Defendants additional time in which to complete their misappropriation of customers' Bitcoin deposits.

91. Defendants' lulling emails of September 11 and 12, 2017, and the lulling Facebook post of September 15, 2017, had their desired effect. Based on these communications by Defendants, many customers did not expect Bitcoin refunds or payments from Defendants until at least the "end of October" or November 2017.

F. Reynolds Was a Controlling Person of Control-Finance

92. At all times, Reynolds was a controlling person of Control-Finance. Reynolds founded and organized Control-Finance, acted as its sole Director, and registered the Internet domain name for the Control-Finance Website. Reynolds either directly or indirectly created content for the Control-Finance Website, opened wallet addresses on behalf of Control-Finance (including CoinPayments Address *uk1x and Ponzi Address *hL1m), operated the Control-Finance Email Address and the Social Media Accounts, and executed fraudulent blockchain transactions on behalf of Control-Finance.

Case 1:19-cv-05631-MKV Document 34-1 Filed 08/20/20 Page 31 of 37

VI. VIOLATIONS OF THE COMMODITY EXCHANGE ACT AND COMMISSION REGULATIONS

Count I—Fraud by Deceptive Device or Contrivance

Violations of Section 6(c)(1) of the Act and Regulation 180.1(a) by Defendants

93. Paragraphs 1 through 92 are re-alleged and incorporated herein by reference.

94. Section 6(c)(1) of the Act, 7 U.S.C. § 9(1) (2012), makes it unlawful for any person, directly or indirectly, to:

> use or employ, or attempt to use or employ, in connection with any swap, or a contract of sale of any commodity in interstate commerce, or for future delivery on or subject to the rules of any registered entity, any manipulative or deceptive device or contrivance, in contravention of such rules and regulations as the Commission shall promulgate by not later than 1 year after [July 21, 2010, the date of enactment of the Dodd-Frank Wall Street Reform and Consumer Protection Act] . . . .

95. Regulation 180.1(a), 17 C.F.R. § 180.1(a) (2018), provides:

> It shall be unlawful for any person, directly or indirectly, in connection with any swap, or contract of sale of any commodity in interstate commerce, or contract for future delivery on or subject to the rules of any registered entity, to intentionally or recklessly:
> (1) Use or employ, or attempt to use or employ, any manipulative device, scheme, or artifice to defraud;
> (2) Make, or attempt to make, any untrue or misleading statement of a material fact or to omit to state a material fact necessary in order to make the statements made not untrue or misleading;
> (3) Engage, or attempt to engage, in any act, practice, or course of business, which operates or would operate as a fraud or deceit upon any person . . . .

96. Bitcoin is encompassed within the definition of "commodity" under Section 1a(9) of the Act, 7 U.S.C. § 1a(9) (2012).

97. As alleged in paragraphs 1-92 above, Defendants violated Section 6(c)(1) of the Act and Regulation 180.1(a) by, among other things, in connection with contracts of sale of

commodities in interstate commerce, (1) using and employing, or attempting to use and employ, manipulative devices, schemes, or artifices to defraud; (2) making or attempting to make untrue or misleading statements of material fact or omitting to state or attempting to omit material facts necessary in order to make the statements made not untrue or misleading; and (3) engaging, or attempting to engage, in any act, practice, or course of business, which operates or would operate as a fraud or deceit upon any person, by, without limitation, the following:

a. issuing written statements misrepresenting that Control-Finance traded customers' Bitcoin deposits on customers' behalf;

b. issuing falsified Trade Reports that reflected virtual currency trades that were never placed and profits that did not exist;

c. issuing written statements misrepresenting that Control-Finance employed professional and specialist virtual currency traders;

d. issuing written statements that falsely represented that Defendants provided customers with risk diversification, asset allocation, and protection from virtual currency market dislocations;

e. issuing written statements that falsely represented that customers' Control-Finance accounts were safe and secure;

f. issuing sham account statements and profit reports that falsely reflected the balances, profits, and interest held in customers' Control-Finance accounts;

g. issuing written statements that falsely represented that depositing Bitcoin with Defendants resulted in guaranteed daily and monthly profits for customers;

Case 1:19-cv-05631-MKV Document 34-1 Filed 08/20/20 Page 33 of 37

h. issuing written statements that falsely represented that Defendants' Affiliate Program generated profits for Affiliates;

i. issuing written statements that falsely represented that Defendants would pay Control-Finance Affiliates escalating bonuses and rewards for referring new customers to Defendants;

j. issuing written statements misrepresenting that Defendants would return customers' principal deposits and account balances by late October or November 2017;

k. misappropriating customers' Bitcoin deposits for Defendants' own use;

l. misappropriating customers' Bitcoin deposits to make Ponzi scheme-like payments to customers who requested account withdrawals;

m. failing to disclose to prospective and existing customers that Defendants misappropriated customers' deposits; and

n. failing to disclose to prospective and existing customers that purported trading profits and returns paid to certain customers were actually the misappropriated principal deposits of other customers.

98. Defendants intentionally or recklessly engaged in the acts and practices alleged above.

99. At all times relevant to this Complaint, Reynolds controlled Control-Finance, directly or indirectly, and did not act in good faith or knowingly induced, directly or indirectly, Control-Finance's conduct constituting the violations of the Act and Regulations described in this Count. Accordingly, pursuant to Section 13(b) of the Act, 7 U.S.C. § 13c(b) (2012),

Case 1:19-cv-05631-MKV Document 34-1 Filed 08/20/20 Page 34 of 37

Reynolds is liable for Control-Finance's violations of Section 6(c)(1) of the Act and Regulation 180.1(a).

100. The acts, omissions, and failures of Reynolds alleged in this Complaint occurred within the scope of his agency, employment, or office at Control-Finance. Accordingly, Control-Finance is liable under Section 2(a)(1)(B) of the Act, 7 U.S.C. § 2(a)(1)(B) (2012), and Regulation 1.2, 17 C.F.R. § 1.2 (2018), as a principal for Reynolds's acts, omissions, or failures in violation of Section 6(c)(1) of the Act and Regulation 180.1(a).

101. Each act of (1) using or employing, or attempting to use or employ, a manipulative device, scheme, or artifice to defraud; (2) making, or attempting to make, untrue or misleading statements of material fact, or omitting to state material facts necessary to make the statements not untrue or misleading; and (3) engaging, or attempting to engage, in a fraudulent or deceitful act, practice, or a course of business, including but not limited to those specifically alleged herein, is alleged as a separate and distinct violation of Section 6(c)(1) of the Act and Regulation 180.1(a).

VII. RELIEF REQUESTED

WHEREFORE, the Commission respectfully requests that the Court, as authorized by Section 6c of the Act, 7 U.S.C. § 13a-1 (2012), and pursuant to its equitable powers, enter:

a. an order finding that Control-Finance and Reynolds violated Section 6(c)(1) of the Act, 7 U.S.C. § 9(1) (2012), and Regulation 180.1(a), 17 C.F.R. § 180.1(a) (2018);

b. an order of permanent injunction prohibiting Control-Finance and Reynolds, and any other person or entity associated with them, from engaging in conduct that violates Section 6(c)(1) of the Act and Regulation 180.1(a);

c. an order of permanent injunction enjoining Control-Finance and Reynolds and any other person or entity associated with them from:

i. trading on or subject to the rules of any registered entity (as that term is defined in Section 1a(40) of the Act, 7 U.S.C. § 1a(40) (2012));

ii. entering into any transactions involving "commodity interests" (as that term is defined in Regulation 1.3, 17 C.F.R. § 1.3 (2018)), for their own personal account(s) or for any account in which they have a direct or indirect interest;

iii. having any commodity interests traded on their behalf;

iv. controlling or directing the trading for or on behalf of any other person or entity, whether by power of attorney or otherwise, in any account involving commodity interests;

v. soliciting, receiving, or accepting any funds from any person for the purpose of purchasing or selling any commodity interests;

vi. applying for registration or claiming exemption from registration with the Commission in any capacity, and engaging in any activity requiring such registration or exemption from registration with the Commission, except as provided for in Regulation 4.14(a)(9), 17 C.F.R. § 4.14(a)(9) (2018);

vii. acting as a principal (as that term is defined in Regulation 3.1(a), 17 C.F.R. § 3.1(a) (2018)), agent, or any other officer or employee of any person (as that term is defined in Section 1a(38) of the Act, 7 U.S.C.

§ 1a(38) (2012)), registered, exempted from registration, or required to be registered with the Commission (except as provided for in Regulation 4.14(a)(9));

d. an order directing Defendants, as well as any successors thereof, holding companies, and alter egos, to disgorge, pursuant to such procedure as the Court may order, all benefits received from the acts or practices which constitute violations of the Act and Regulations, as described herein, and pre- and post-judgment interest thereon from the date of such violations;

e. an order directing Defendants, as well as any successors thereof, to make full restitution to every person or entity whose Bitcoin they received or caused another person or entity to receive as a result of acts and practices that constituted violations of the Act and Regulations, as described herein, and pre- and post-judgment interest thereon from the date of such violations;

f. an order directing Defendants, as well as any successors thereof, holding companies, and alter egos, to rescind, pursuant to such procedures as the Court may order, all contracts and agreements, whether implied or express, entered into between them and any customers whose Bitcoin were received by them as a result of the acts and practices which constituted violations of the Act and Regulations, as described herein;

g. an order directing each Defendant to pay a civil monetary penalty, to be assessed by the Court, in an amount not to exceed the penalty prescribed by Section 6c(d)(1) of the Act, 7 U.S.C. § 13a-1(d)(1) (2012), as adjusted for inflation pursuant to the Federal Civil Penalties Inflation Adjustment Act Improvements

Act of 2015, Pub. L. 114-74, 129 Stat. 584 (2015), tit. VII, § 701, and Regulation 143.8, 17 C.F.R. § 143.8 (2018), for each violation of the Act and Regulations, as described herein;

h. an order requiring Defendants to pay costs and fees as permitted by 28 U.S.C. §§ 1920 and 2412(a)(2) (2012); and

i. an order providing such further relief as the Court deems just and proper.

* * *

Dated: June 17, 2019

Respectfully submitted,

COMMODITY FUTURES TRADING COMMISSION

s/Jonah E. McCarthy

Daniel J. Grimm (*pro hac vice* application to be submitted)
Senior Trial Attorney
dgrimm@cftc.gov

Jonah E. McCarthy (S.D.N.Y. Bar No. JM1977)
Senior Trial Attorney
jmccarthy@cftc.gov

Luke B. Marsh (*pro hac vice* application to be submitted)
Chief Trial Attorney
lmarsh@cftc.gov

Paul G. Hayeck (*pro hac vice* application to be submitted)
Deputy Director
phayeck@cftc.gov

COMMODITY FUTURES TRADING COMMISSION
Division of Enforcement
1155 21st Street, N.W., Washington, DC 20581
Telephone: (202) 418-5000
Facsimile: (202) 818-3179
Attorneys for Plaintiff